# CLAIMS

What is claimed is:

1. A method for behavior based access tracking of an application comprising:

intercepting an access attempt to a protected resource;

comparing the access attempt to a preexisting set of allowable access attempts to determine if the access attempt corresponds to a previous allowable access;

selectively permitting, based on the comparing, access to the protected resource according to the access attempt; and

augmenting the set of allowable access attempts by selectively adding, based on inferential feedback, the access attempt to the set of allowable access attempts.

2. The method of claim 1 wherein comparing the access attempt determines correspondence by a matching of explicit rules qualifying allowable data access attempts and by a matching of a baseline having previously allowed data access attempts

3. The method of claim 1 wherein adding further comprises selectively adding, if the data access transaction corresponds to a window of allowable database activity, the data access attempt to the set of allowable data access attempts.

4. The method of claim 1 wherein comparing the access attempt to preexisting access attempts comprises:

determining a structure of the access attempt corresponding to syntactical arrangement of the access attempt; and

comparing the determined structure of the access attempt independently of the data values implicated in the access attempt.

5. The method of claim 4 wherein comparing the determined structure further comprises comparing a hash value derived from the determined structure.

6. The method of claim 4 wherein determining the structure further comprises:

parsing the access attempt; and

building a parse tree from the parsing, the parse tree indicative of a syntactical structure of the data access attempt, wherein comparing further comprises computing a hash value from the parse tree, and comparing the hash value to the hash values of previous access attempts.

7. The method of claim 1 further comprising defining an access policy having a plurality of access rules, the access rules indicative of allowable access, wherein the preexisting set of allowable access attempts correspond to one of the plurality of the rules.

8. The method of claim 1 wherein determining the preexisting set comprises establishing a baseline of allowable activity, the baseline indicative of an accepted set of allowable access attempts.

9. The method of claim 8 wherein the baseline is a rule in the access policy and indicates allowable access when a data access transaction matches a previous data access transaction represented in the baseline.

10. The method of claim 8 wherein the baseline includes structure the of the access attempts, and avoids including data values of the data access transactions from which it is derived

11. The method of claim 1 wherein selectively permitting further comprises computing, based on iteratively applying the access rules to the access attempt, an access result indicative of whether to allow the access attempt.

12. The method of claim 1 further comprising:

identifying a plurality of allowable access attempts;

inferring, based on observable patterns in the allowable access attempts, access rules indicative of the plurality of allowable access attempts; and

adding the inferred rules to the access policy.

13. The method of claim 12 wherein inferring further comprises:

processing the series of allowable access attempts to determine related groups of allowable access transactions;

suggesting, based on a commonality of the processed group of allowable access attempts, an access rule indicative of each of the series of allowable access attempts; and

adding, in response to operator input, the suggested access rule to the access policy.

14. The method of claim 1 wherein the preexisting set of allowable access attempts comprise a current baseline representative of a window of access attempts, further comprising modifying the current baseline by including access attempts from a different window of access attempts.

15. The method of claim 11 wherein adding further comprises:

identifying a sampling window of access attempts, the sampling window deterministic of allowable access patterns to the protected resource;

storing an indication of the access attempts made during the window of access attempts; and

merging the window of access attempts with the current baseline set of access attempts, the current baseline deemed deterministic of allowable access behavior.

16. The method of claim 1 wherein storing further comprises:

verifying that the access attempt is indicative of allowable access behavior; and

selectively adding, based on the verifying, the access attempts to the baseline of allowable access attempts.

17. The method of claim 16 wherein determining the preexisting set includes comparing a sensitivity threshold indicative of a series of corresponding access attempts defining a benign pattern.

18. The method of claim 17 wherein the corresponding access attempts define a similar pattern of access structures, the access structures determined by tables and fields affected by the access attempt.

19. The method of claim 7 wherein the parse tree further conforms to a platform independent format, wherein parse trees and corresponding hash values generated from different platforms are similar and are operative to result in a consistent comparison result for similar data access attempts on a plurality of platforms.

20. The method of claim 1 further comprising:

storing a set of data access attempts according to a learning window of observable database behavior;

generating suggested rules;

adding suggested rules to the security policy; and

reanalyzing the set of data access attempts gathered during the leaning window in an iterative manner against suggested rules.

21. A security filter device for behavior based access tracking of a software application comprising:

a database access analyzer operable to intercept an access attempt to a protected resource;

a baseline comparator operable to compare the access attempt to a preexisting set of allowable access attempts to determine if the access attempt corresponds to a previous allowable access attempt;

an enforcer operable to selectively permit, based on the comparing, access to the protected resource according to the access attempt; and

an inference engine operable to add, if the access attempt is permitted, the access attempt to the set of allowable access attempts.

22. The security filter device of claim 21 wherein the baseline comparator is further operable to comparing the access attempt and determine correspondence by matching explicit rules qualifying allowable data access attempts and matching of a baseline having previously allowed data access attempts.

23. The security filter device of claim 21 further comprising:

a parser in the database access analyzer operable to determine a structure of the access attempt corresponding to syntactical arrangement of the access attempt, wherein the baseline comparator is operable to compare the determined structure of the access attempt independently of the data values implicated in the data access attempt.

24. The security filter device of claim 23 wherein the database access analyzer further includes a hash engine operable to compute a hash value derived from the determined structure.

25. The security filter device of claim 23 wherein the parser is further operable to:

parse the access attempt; and

build a parse tree from the parsing, the parse tree indicative of a syntactical structure of the data access attempt, wherein the baseline comparator is operable to compare the computed hash value from the parse tree to the hash values computed from previous access attempts.

26. The security filter device of claim 21 further comprising an access policy having a plurality of access rules, the access rules indicative of allowable access, wherein the preexisting set of allowable access attempts correspond to one of the plurality of the rules.

27. The security filter device of claim 21 wherein the preexisting set further comprises a baseline of allowable activity, the baseline indicative of an accepted set of allowable access attempts.

28. The security filter device of claim 27 wherein the parser is operable to generate a parse tree corresponding to the structure of the access attempts, the parse tree not including data values of the data access transactions from which it is derived.

29. The security filter device of claim 21 wherein the inference engine is operable to:

identify a plurality of allowable access attempts; and

infer, based on observable patterns in the allowable access attempts, access rules indicative of the plurality of allowable access attempts; and

add the inferred rules to the access policy.

30. The security filter device of claim 29 wherein the inference engine further comprises:

a learner operable to process the series of allowable access attempts to determine related groups of allowable access transactions, the learner further operable to suggest, based on a commonality of the processed group of allowable access attempts, an access rule indicative of each of the series of allowable access attempts; and

a rule suggestor operable to add, in response to operator input, the suggested access rule to the access policy.

31. The security filter device of claim 21 wherein the preexisting set of allowable access attempts comprise a current baseline set representative of a window of access attempts, wherein the inference engine is operable to modify the current baseline by including access attempts from a different window of access attempts.

32. The security filter device of claim 31 wherein the inference engine is further operable to:

identify a sampling window of access attempts, the sampling window deterministic of allowable access patterns to the protected resource;

store an indication of the access attempts made during the window of access attempts; and

merge the window of access attempts with the current baseline set of access attempts, the current baseline deemed deterministic of allowable access behavior.

33. The security filter device of claim 21 wherein the inference engine is further operable to:

retain the data access attempts during a learning window of observable database behavior;

generate suggested rules based on the learning window;

conditionally add suggested rules to the security policy; and

reanalyze the set of data access attempts gathered during the leaning window in an iterative manner against suggested rules.

34. The security filter device of claim 21 wherein the rule logic in the inference engine is further operable to:

verify that the access attempt is indicative of allowable access behavior; and

selectively add, based on the verification, the access attempts to the baseline of allowable access attempts.

35. The security filter device of claim 34 wherein determining the preexisting set includes comparing a sensitivity threshold indicative of a series of corresponding access attempts defining a benign pattern.

36. The security filter device of claim 35 wherein the corresponding access attempts define a similar pattern of access structures, the access structures determined by tables and fields affected by the access attempt.

37. The security filter device of claim 21 further including an interface operable with an external application, the interface operable to transmit allowable data access attempts to the external application.

38. The security filter device of claim 21 wherein the database analyzer further includes an interface operable with an external application, the database analyzer operable for receiving data access attempts from the external application via the interface, process the received data access attempts, and forwarding the processed data access attempts to the security filter and the repository for processing via the inference engine.

39. A computer program product having a computer readable medium operable to store computer program logic embodied in computer program code encoded thereon for behavior based access tracking of a software application comprising:

computer program code for intercepting an access attempt to a protected resource;

computer program code for comparing the access attempt to a preexisting set of allowable access attempts to determine if the access attempt corresponds to a previous allowable access attempt;

computer program code for selectively permitting, based on the comparing, access to the protected resource according to the access attempt; and

computer program code for adding, if the access attempt is permitted, the access attempt to the set of allowable access attempts.

40. A computer data signal having program code for behavior based access tracking of a software application comprising:

program code for intercepting an access attempt to a protected resource;

program code for comparing the access attempt to a preexisting set of allowable access attempts to determine if the access attempt corresponds to a previous allowable access attempt;

program code for selectively permitting, based on the comparing, access to the protected resource according to the access attempt; and

program code for adding, if the access attempt is permitted, the access attempt to the set of allowable access attempts.

41. A security filter device for behavior based access tracking of a software application comprising:

means for intercepting an access attempt to a protected resource;

means for comparing the access attempt to a preexisting set of allowable access attempts to determine if the access attempt corresponds to a previous allowable access attempt;

means for selectively permitting, based on the comparing, access to the protected resource according to the access attempt; and

means for adding, if the access attempt is permitted, the access attempt to the set of allowable access attempts.